

«Интернет – угрозы –  
кибербезопасность»

## Пояснительная записка

**Актуальность.** В наш век компьютерных технологий и скоростного Интернета, В век информационной среды, которая развивается огромными темпами, дети разных возрастов всё свободное время проводят в социальных сетях, они общаются, играют, учатся, читают, добывают разнообразную информацию. При этом они подвергаются большой опасности, о которой не всегда подозревают. Это несёт угрозу здоровью и психике учащихся.

Проблема кибербезопасности учащихся является одной из основных в воспитательном процессе. Более 90% пользователей сталкивается с киберугрозами в сети, но не каждый может с ними справиться. Чтобы обезопасить детей, необходимо повышать информационную грамотность не только среди детей, но и среди учителей, воспитателей, родителей и всех участников образовательного процесса.

Таким образом, данная тема очень актуальна, так как поможет ребятам обезопасить себя и своих родных путём устранения угроз, которые исходят из сети Интернет, и знаниями о кибербезопасности.

**Целевая аудитория:** 6-9 классы (12-15 лет)

- **Цель:** Расширение знаний учащихся о киберугрозах; формирование навыков их распознавания и оценки рисков; обеспечение информационной безопасности учащихся путем привития им навыков ответственного и безопасного поведения в среде Интернет.
- **Задачи:**
  - -познакомить учащихся с основными рисками использования Интернета и путях их устранения;
  - - дать определение понятиям: фишинг, СПАМ и СМС, кибербуллинг, кража личности;
  - - воспитывать информационную культуру личности.

Планируемые результаты:

**Предметные:** сформулировать представление о киберугрозах, развивать умение предотвратить их, формировать навык защиты от киберугроз.

**Личностные:** понимать социальную, общекультурную роль в жизни современного человека навыков ответственного и безопасного поведения в среде Интернет.

**Метапредметные:** формировать умения и навыки безопасного использования средств развития информационных и коммуникативных технологий, развитие и обеспечение информационной грамотности.

**Форма проведения:** эвристическая беседа с использованием видеоролика, анализ информации, групповая и индивидуальная работа.

**Педагогическая технология: смешанная:** компьютерная технология, игровая, групповая, здоровьесберегающая.

**Методы и приемы:** беседа, тестирование, онлайн-игра-практическая работа, видеометод.

**Ресурсы:** компьютеры, мультимедийный проектор, видеоролик, презентация, чек-лист для саморефлексии.

## Ход мероприятия

Этапы	Содержание	Деятельность учителя	Деятельность обучающихся
Мотивационный	<p>Формулирование учащимися темы урока</p> <p>Формулирование цели мероприятия</p>	<p>Прежде, чем начнем наше мероприятие, предлагаю вам разгадать ребусы и определить тему нашего занятия. (Слайд _)</p> <p>Можете назвать тему урока? (Слайд _)</p> <p>Чтобы вы назвали цель занятия, предлагаю вам посмотреть видеоролик (Слайд _)</p> <p>Сформулируйте цели нашего занятия (Слайд _)</p>	<p>Учащиеся разгадывают слова: Интернет, угроза, кибербезопасность</p> <p>Учащиеся формулируют тему занятия</p> <p>Учащиеся смотрят видеоролик</p> <p>После просмотра учащиеся формулируют цель занятия.</p>
Деятельностный	Проверка уровня зависимости от Интернета (выполнение теста)	<p>- Сегодня я хочу поговорить с вами о вашей активности в Интернете, о том, какие угрозы подстерегают вас в это время и о правилах кибербезопасности и защиты от угроз.</p> <p>Но вначале прошу вас пройти тест на проверку вашей зависимости от Интернета (Слайды ___)</p>	<p>Учащиеся отвечают на вопрос.</p> <p>Учащиеся выполняют задание, подсчитывают количество баллов.</p>
		- Я вижу, что вы проводите много времени в социальных сетях, а знаете ли вы об опасностях, которые вас там поджидают?	Учащиеся перечисляют киберугрозы.
	Работа с презентацией	<p>Проверка усвоения увиденного.</p> <p>- Каким словом называются информационные угрозы?</p> <p>- Как называют методы борьбы с ними?</p> <p>- Как вы понимаете это слово? (Слайд __)</p>	<p>Учащиеся смотрят презентацию и делают записи.</p> <p>Учащиеся отвечают: Киберугрозы. Кибербезопасность</p> <p>Кибербезопасность – это умение оценить достоверность информации, умение сохранить свои личные и персональные данные, умение защищать свои и не нарушать чужие авторские права.</p>
		<p>- Когда вы заходите в Интернет, вы предоставляете доступ к своим личным данным, а цифровые устройства наблюдают за вами и фиксируют информацию. Любые передвижения в Интернете отслеживаются.</p> <p>- Как вы думаете, для чего ведется такой сбор информации о пользователях Интернета?</p>	<p>Ученики отвечают: - Персональные данные интересуют разных разработчиков и рекламщиков, а также разных мошенников.</p>

		<p>- С какими же угрозами мы сталкиваемся в Интернете?</p>	<p>Ответы учащихся:</p> <ul style="list-style-type: none"> <li>- Фишинг</li> <li>- СПАм и СМС</li> <li>- Кибербуллинг</li> <li>- Кражи личности</li> </ul>
Продолжаем изучать презентацию	<p>Рассмотрим инфографику, представленную на презентации (Слайд ___)</p> <p>- Что такое фишинг?</p> <p>- Фишинговые сайты внешне ничем не отличаются от официальных. Их несложно отличить от официальных. Например, vkontaktte.</p> <p>- Как вы думаете, сайт официальный или нет?</p> <p>- Вам необходимо скачать браузер Chrome. С какого сайта вы его будете скачивать?</p> <p>- Как вы узнаете официальный сайт или нет?</p> <p>Верно, такой сайт более защищенный, чем http, потому что мошенникам нет дела до получения сертификата.</p> <p>- Если вы попадетесь на обман, что необходимо сделать? (Слайд __)</p>	<p>Ответы учащихся:</p> <ul style="list-style-type: none"> <li>- Это несанкционированный доступ к паролям и логинам, мошенничество, связанное с поддельными или несуществующими сайтами, которые копируют официальные сайты банков, социальных сетей.</li> </ul> <p>Учащиеся отвечают:</p> <ul style="list-style-type: none"> <li>- Нет, так как в адресе есть лишняя буква <b>t</b>.</li> <li>- С любого или официального.</li> <li>- Адрес должен начинаться с протокола https.</li> <li>- Срочно менять пароль в официальной записи сайта.</li> </ul>	
	<p>Следующий вид киберугроз - это Спам- или смс-мошенничество.</p> <p>Приходили ли к вам такие письма? Как вы поступаете в таком случае?</p> <p>Как нужно поступить, когда приходят такие письма? (Слайд __)</p>	<p>Ответы учащихся:</p> <ul style="list-style-type: none"> <li>- Предложение отправить сообщение на короткий номер, согласие на рассылку.</li> <li>- Не отвечать, удалять, проверять сообщения, позвонив родным.</li> </ul>	
	<p>- Что такое кибербуллинг? (Слайд ___)</p> <p>- Кибербуллинг – уголовно наказуемое преступление. Что нужно делать, если вы подверглись кибербуллингу?</p> <p>- сбор фактов, сохранение, распечатка доказательств для обращения в полицию;</p> <p>- использовать функцию блокировки;</p> <p>- никогда не стоит следовать требованиям, вступать в переговоры или пытаться откупиться;</p> <p>- не пытайтесь бороться с угрозами в одиночку, необходимо сообщить родителям.</p>	<p>Кибербуллинг = это подростковый виртуальный террор и давление на жертву, связан с унижением и оскорблением, угрозами в социальных сетях.</p> <p>Ответы учеников:</p> <ul style="list-style-type: none"> <li>- сбор фактов, сохранение, распечатка доказательств для обращения в полицию;</li> <li>- использовать функцию блокировки;</li> <li>- никогда не стоит следовать требованиям, вступать в переговоры или пытаться откупиться;</li> <li>- не пытайтесь бороться с угрозами в</li> </ul>	

			одинокую, необходимо сообщить родителям.
		- Что делать при краже личности?	- То же самое, что и при смс мошенничестве.
Итогово-рефлексивный		Подводим итог: - Не переходить по подозрительным ссылкам; - скачивать приложения только с официальных сайтов; - не переводить деньги в подозрительные организации; - игнорировать подозрительные смс и спамы; - не поддаваться оскорблениям и унижениям в сети Интернет.	
Физкультминутка		При работе за компьютером мы не должны с вами забывать и о безопасности своего здоровья. Сейчас я предлагаю вам выполнить физкультминутку для глаз. Ваша задача следить, что происходит на экране.	Учащиеся смотрят на экран.
	Практическая работа	Мы с вами хорошо поработали. Надеюсь, сумеете обнаружить угрозы и обезопасить себя и свои данные. Для этого всего лишь необходимо соблюдать основные правила безопасности. Чтобы закрепить ваши знания пройдем онлайн-игру «Кибербезопасность в сети Интернет» <a href="https://safe.mail.ru/test">https://safe.mail.ru/test</a> (Слайд ___)	Учащиеся рассаживаются за компьютерами и по ссылке заходят на сайт и выполняют задания.
	Рефлексия	Прежде чем завершить наше мероприятие, прошу вас ответить на вопросы чек-листа. Ребята, сегодня мы говорили о том, с какими неприятностями сталкиваетесь вы при работе с Интернетом, предлагаю вам памятку правила безопасности. Надеюсь, наше мероприятие принесет вам пользу, и вы будете следовать вашим правилам. Будьте всегда осторожны и бдительны! Спасибо за работу! Вы молодцы!	Учащиеся получают распечатанный чек-лист  Учащиеся получают памятку